A LITERATURE REVIEW ON DATABASE CYBER SECURITY: ATTACKS, COUNTERMEASURES AND TECHNIQUES

Syed Arif Islam, M. Mohankumar*

Abstract

With the latest technology, people generate a large amount of data by utilizing various programs, which are transferred to store in a database. Data is maintained and changed in this cyber database system. Because such a large amount of data is saved in the database that must be safeguarded. Cyber security is safeguarding and protecting data and databases against illegal access threats and attacks. As the database's complexity develops, so different types of threats and attacks increase. Therefore, security becomes critical. A result of this paper shows numerous threats and attacks. By Presenting some countermeasures, that will fortify and secure the cyber database. Various database cyber security techniques are described in this paper so the database will be safer and more reliable.

Keywords: database; cybersecurity; attacks; threats; countermeasures; techniques

I INTRODUCTION

A database is like a collection of data or information that has been arranged in such a way that it can be easily accessed, controlled, and updated. In the cyber world, databases are sometimes classified, according to the organisational techniques with a relational database, which is a data representation that is smooth being one of the most frequent approaches [1]. The data is structured in such a way that it may be reorganised and accessed in a variety of cyberattacks. It can be disclosed or copied among different nodes in a network in a distributed database.

Any authorised user can enter quickly and easily access, and analyse the data in cyber databases. It consists of a set of views, tables, and queries. The information that is saved in the databases is normally organised in facilitating the procedures, that necessitate the storage and retrieval of data. The Database Management System (DBMS) is a computer programme that manages all databases that are currently stored on any hard drive or network. The database is where the system's vital information is kept. As a consequence, the security of cyber databases cannot be disregarded. The process of preserving sensitive and secret data contained in a database is known as cyber database security. Cyberattacks are becoming more common and threatening, and the attackers are more determined and sophisticated [2]. It is also likely to be linked to a country state, which is why it is so threatening. Existing database countermeasures, such as security tools and processes, are insufficient [3]. Its purpose is to protect databases at all levels from unauthorised or unlawful access or threats.

II LITERATURE REVIEW

In this field, there is a significant quantity of work. For this article, we have reviewed and used the following reference.

Marco Angelini, Claudio Ciccotelli1, , Luisa Franchina , Alberto Marchetti-Spaccamela, and Leonardo Querzoni

Cyber threats and attacks take advantage of the growing problem, putting vital infrastructure systems, security, the financial sector, and human safety and well-being in danger. Cybersecurity risk affects a company's financial and reputational risk, and it can drive up expenses and negatively influence sales. It has the potential to undermine an organization's ability. As a result, the average cost of

Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
*Corresponding Author

cybercrime is going up, and current spending priorities often don't work as well as they should [4].

Christopher Kuner, Dan Jerker B. Svantesson, Fred H. Cate, Orla Lynskey and Christopher Millard

Historically, many data protection specialists in industry and government lacked familiarity with the technology. Following major terrorist attacks, governments think about, and in many cases adopt, private-restrictive policies because they think that giving up a little privacy for more security is worth it, even if it means giving up some privacy. This is beginning while focus too much on cybersecurity [2].

Sohail IMRAN, Irfan Hyder

The authors of this study explored several security challenges and models for various database management systems. The paper makes several recommendations for security models for traditional databases and object-oriented systems that are both discretionary and obligatory. Despite this, there is no set of recommendations for developing security models. This study provides a consolidated picture of database security by offering a consolidated image of different database security problems. It can be used to establish, design, and implement a database security policy that is effective [5].

Simanta Shekhar Sarmah

The protection of data is critical. It influences the economic activities of businesses and the public's trust in government. Internal personnel accounts for about 25% of incidents, with loss or theft of various equipment accounting for 50%. The concept of a penetration database is explained in this article, as well as how to ensure compliance. For good database security, take strategic and technical security measures [6].

V. Pevnev, S. Kapchynskyi

This article tries to explain the concept of data security by providing a comprehensive set of rules and activities that might reduce the risks associated with data confidentiality, integrity, and availability violations. It also discusses several types of vulnerabilities that can arise when using current databases and database management systems. While developing, managing, and using databases, the use of the provided advice will help to avoid the impact of the threats. Various insider risks, in particular, that constitute a sufficiently substantial niche in the list of database threats [7].

III. CYBER THREATS AND ATTACKS OF DATABASE

Because databases hold sensitive information, they are vulnerable to a variety of threats and attacks. The threats and attacks are classified as follows:

A. Excessive Database Privileges.

Database management systems and their accompanying data structures are complex, administrators provide users excessive permissions to avoid application failure due to a lack of permissions [1]. When users are given more rights than are necessary for their job functions, these powers might be abused [6]. For example, any university course coordinator has the authority to post each student's grades. This permission can be abused to alter any student's or subject's grades. This abuse occurs, as a result of giving a specific group of users generic access rights.

B. Mobile Cyber Device Attacks

Many businesses are seeking to expand employee mobility because it boosts operational efficiency and productivity. However, hackers are well aware of this reality and they are increasingly targeting mobile devices with a range of attacks, putting enterprises in danger of a data breach through more devices than ever before [8]. A good example is the Pegasus attack against Apple's iOS software. Pegasus affected iPhones by sending phishing text messages

that asked recipients to click on a link embedded in the message. The installation of malware capable of monitoring people through their camera and microphone was activated by clicking the link. User's login credentials for WhatsApp, Gmail, and other important communication apps were taken once they were infected.

C. Attacks on Credential Stuffing

Credential stuffing is a form of brute-force cyber-attack in which criminals utilise stolen usernames and passwords from one data breach to gain access to user accounts at another [9]. Credential stuffing is possible since 65 % of people use the same password for many accounts, according to statistics. As a result, credential stuffing is one of the most common causes of data breaches all around the world.

D. Database Backups Exposure.

Backup storage media are regularly subjected to unprotected attacks. As a result, several security events have resulted in database backups being stolen. Failure to audit and monitor administrators with low-level access to vital data can also put data in danger.Taking the appropriate precautions to safeguard sensitive data backup copies and monitor the majority of highly privileged individuals is not only wise but also mandated by various laws [10].

E. SQL Injections

The backend functionality is contained in database systems.User-supplied data is widely used as input for dynamically generating SQL queries that directly update databases [10]. Input injection is a form of attack that seeks to deviate from the application's original goal by sending attacker-SQL statements were sent straight to the database backend.

There are two forms of input injection:

- SQL Injection: This is a type of attack that targets traditional database systems. Unauthorized statements are frequently inserted into application input areas in its attacks [11].

- NoSQL Injection: NoSQL Injection is aimed at big data systems. In this type of attack, malicious words are injected into big data components like Hive and MapReduce.

F. Denial of Service (DoS) Attack

A DoSattack is a type of cyber-attack. This kind of attack degrades the performance of a database server, and it may become unavailable to all users [12]. Despite the point that a DoS attack does not reveal the contents of a database, it can cost the victims a significant amount of both money and time.

G. Unmanaged Sensitive Data

Data that has been left unmanaged and sensitive. Many companies store sensitive information. Hackers may go after data that has been ignored or disregarded. Additionally, crucial data is constantly uploaded, making it tough to keep track of everything. This means that newly submitted data could be at risk of being hacked.

H. Absence of Security Expertise and Education

Information bases are penetrated and spilled because of non-specialized representatives' absence of IT security information and instruction, making them inclined to breaking fundamental data set security administers and setting data sets in danger. IT safety crew may likewise do not have what it takes needed to carry out safety efforts, implement approaches, and react to incidents.

I. Database Vulnerabilities and Misconfigurations

Due to misconfiguration, databases are frequently determined to be completely hazardous. Also, some databases include accounts and settings which have already been configured. It's vital to keep in mind that hackers are frequently highly experienced IT experts who are well-

versed in exploiting database faults and misconfigurations to launch an attack.

J. Weak Audit Trail

As far as consistency, prevention, discovery, criminology, and recuperation, an absence of review strategy and innovation represents a danger [7]. In any data set organization, exchanges including sensitive information ought to be consequently logged [13]. Inability to keep nitty gritty review records of information base activities is a genuine hierarchical danger on various levels [14]. Data set examining arrangements that are ineffectual will be found disregarding industry and unofficial laws all the more oftentimes. Most review instruments have no thought who the endclient is becausethe activity of any kind is identified with the web application account name. Because of the absence of a relationship to the record client, announcing, perceivability, and legal examination are completely compelled. At last, people having information base head advantages, regardless of whether legitimate or criminal, can impair local data set reviewing to cover deceitful conduct. To ensure fruitful centralization of obligations arrangements, review capacities and obligations ought to ideally be disengaged from both information base directors and the data set server stage.

K. Malware

Malware is a broad term that encompasses a variety of harmful software meant to penetrate, spy on or construct a backdoor into a company's systems or data. Ransomware, worms, trojans, adware, and spyware are all examples of malware. Malware usage has increased by about 80% since early 2020, according to experts. Malware can cause big data breaches and corporate operations to be severely disrupted. WannaCry, a ransomware attack that took use of a flaw in the Microsoft operating system, hit the company hard.

L. Spraying on Password Attacks

Password spraying is a form of brute-force attack in which hostile actors try to guess a user's password by using a list of commonly used passwords such as "123456" or "password."

Password spraying, like credential stuffing, is quite prevalent. According to verizon's 2020 data breach report, brute-force methods like password spraying were used in over 80% of all hacking-related data breaches.

M. Back Door

A backdoor is a type of malware that gains access to a system by circumventing regular authentication methods.As a result, application resources such as databases and file servers can be accessed remotely. Allowing thieves to run system commands and update malware from afar. The installation of a backdoor is done by taking advantage of vulnerabilities in a web application. Due to the encryption of files, detection is difficult once have been deployed. Webserver backdoors are used for a variety of malevolent objectives, including:

- Theft of information.
- Defacement of a website
- Hijacking of a server.
- DDoS (Distributed Denial of Service) attacks are launched.

IV COUNTERMEASURES

A countermeasure of best practices and internal control is required to properly safeguard databases. The following are some of the countermeasures:

A. Excessive Database Privileges

Countermeasures:

- Role-based admittance restrictions inside the software that guide required admittance authorizations to work capacities.

- Procedures to ensure that when representatives change occupations, their authorizations are refreshed and those that are as of now not needed are disavowed.

- Periodic, albeit not generally standard, reviews of who is responsible for explicit situations to guarantee that conventions are being followed and that the worker for hire who left a half year prior doesn't have a functioning record.

B. Mobile Device Attacks

Countermeasures:

To defend software firms from mobile security threats. It needs a solid enterprise mobility management programme and mobile device management technologies, which will help to protect any company data that may be on workers' personal or work devices. Multi-factor authentication and other identity and access management systems can help secure any work applications that hold sensitive data from unwanted access.

C. Attacks on Credential Stuffing

Countermeasures:

Passwordless authentication or Multi-Factor Authentication (MFA) are the best ways to protect against credential stuffing attacks. MFA requires bad actors to prove their identity in one or more ways in addition to the stolen credentials are using to log in, whereas password-less authentication stops bad actors from using stolen credentials by removing them entirely.

D. Database Backups Exposure

Countermeasures:

- For both databases and backups, encryption should be employed. The security of both the production and backup versions of databases is ensured by data encryption. Data encryption is the most effective method for accomplishing this.

- Examine both the database and the backups. This allows administrators to see who has tried to access sensitive data.

E. SQL Injections

Countermeasures:

- In the applications, don't use dynamic queries. By employing prepared statements with parametrized queries, SQL injection can be avoided.

- Before delivering user input to the application, make sure it is valid. This is a very handy additional protection that can also be used to deflect a variety of different attacks.

- As a little something extra, incorporate observing and alarming at the information level for any utilization of dynamic questions. This will stop an attacker from requesting the database directly after bypassing the application.

- Remember that NoSQL information bases are helpless against infusion attacks too; to restrict the danger, safeguards, for example, severe info approval is required.

F. Denial of Service Attack

Countermeasures:

Because DoS attacks are typically difficult to distinguish from normal traffic, they are difficult to detect. Blocking all traffic for a brief period, rate-limiting traffic to a website, utilising a web application firewall to identify suspicious traffic patterns, or spreading traffic across a network of servers are all ways to countermeasures of a DoS attack.

G. Unmanaged Sensitive Data

Countermeasures:

- The database's sensitive data should be encrypted at all times.

- Put on the relevant database permissions and controls.
- Regularly search databases for new sensitive information. In this case, a periodic data discovery and compliance manager that can detect and preserve freshly uploaded sensitive data could be quite valuable.

H. Absence of Security Expertise and Education

Countermeasures:

- Database users must be trained on database security.
- IT security professionals will be challenged to improve their skills and qualifications.

I. Database Vulnerabilities and Misconfigurations

Countermeasures:

- The IT crew should be well-trained and competent, and there should be no default accounts in the databases.

J. Weak Audit Trail

Countermeasures:

- Consider what data will be collected at the application and database query layers. considered system use cases, as well as misuse incidents and the data required to detect them. It is much better ifadd automatic alerting rules.

- Consider how to safeguard any data logging. If everything is kept in a software database, an attacker could erase or distort the log data if the database is compromised. Keep logs to a bare minimum and log data secure because they can include critical information.

- Establish mechanisms for auditing the data collected so that problems can be identified. Examine whether logged data can be shown in a useful manner.

- Think about if network-based audit appliances, which track all database requests at a granular level and are independent of all users, could be justified.

K. Malware

Countermeaures:

Teach employees how to recognise strange links and pop-ups that could contain malware to help limit the risk of infection. Keeping operating systems up to date to ensure known security flaws are fixed and installing anti-virus software are two other ways to defend from malware. For example, the Equifax data leak could have been avoided if a known fix had been applied promptly.

L. Spraying on Password Attacks

Countermeasures:

Password spraying attacks, like credential stuffing attacks,can be mitigated by employing password-less authentication or MFA. However, by adopting the NIST Password Guidelines, which are widely regarded as the highest password standards in the world.It can limit the danger and consequences of a data breach caused by password spraying.

M. Back Door

Countermeasures:

- It is necessary to utilise anti-virus software.
- Installing a network monitoring tool.
- Creating a system for detecting malicious software on endpoints.
- Using a host firewall to ensure that every device is secured.

V DATABASE CYBER SECURITY TECHNIQUES

Any organizations backbone is its database. As a result, any cyber security solution must be implemented by the business. Not only the data inside the system but also the database hardware, software,and human resources, must be protected by the cyber security technique.

A. Controlling Access

The communications between databases and other well-known devices are managed via access control.

Unauthorized users are unable to harm databases either internally or externally and databases are secured from potential faults. The organisation system can be impacted by large mistakes problems.

Maintaining access control helps to prevent hazards and safeguard data in an organizations system. For example, if someone destroyed a data table or stooled data organisation, the system could collapse but this problem could be overcome by implementing access control.

B. Resilience of Data

Systems will be able to withstand or recover from failures if theyhave perfect data security. By incorporating resiliency into the hardware and software, it can ensure that security is not jeopardised by events like power outages or natural catastrophes.

C. Detecting Anomaly

Detecting network abnormalities can be difficult without a baseline understanding of how the network should behave. Anomaly Detection Engines (ADE) provides network analysis so that when security breaches occur, the network can be warned promptly enough to respond.

D. Accountability and Auditing

Accountability and audit ensure the physical integrity of data, which could be addressed through auditing records. User's accounting and access are analysed using auditing and accountability.

E. Verification

The term "simple authentication" refers to who is allowed access to the network. Authentication can be used to determine which users are permitted to access databases. It is authenticated to protect sensitive data from unauthorised parties.

- Combination of user name and password.
- Questions to challenge and respond to
- Token cards are used to represent something else.

F. Encryption

Cryptography is a technology that helps secure data from unauthorised access. Encryption is a technique used in cryptography. The process of converting plaintext to ciphertextis known as encryption. This ciphertext is unreadable and unintelligible to the average person. Encrypted data is the name given to this ciphertext [15] [16] [17]. This encryption employs two different sorts of encryption techniques.Database Encryption and Application Layer Encryption.

- **Encryption of Databases**

An addon is a term used to describe a database encryption relationship. Encryption is applied to data before it is stored in a database. All encryption and key management can take place on the database server without the awareness of the users. Database encryption is simpler to implement but it must be protected against hostile parties.

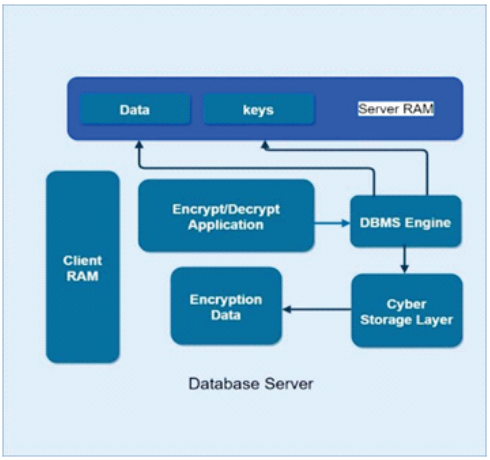

Fig.1 Database Encryption

- **Encryption at the Application Layer**

Data can be encrypted before being stored on a credit card. Before storing data in the file system or databases, the application must encrypt the data. Before data can be shown,

applications must decrypt it. The user understands how to use encryption and decryption in the application layer. Depending on the logic of the application, multiple algorithms and key management systems might be used.

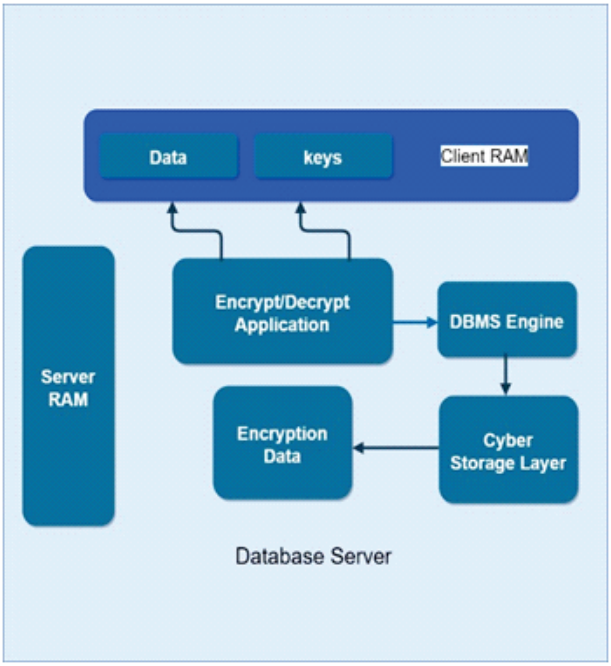

Fig.2 Application Layer Encryption G Asymmetric Key Algorithm and Symmetric Key Algorithm

G. Asymmetric Key Algorithm and Symmetric Key Algorithm

Asymmetric encryption algorithms, often known as public-key algorithms, encrypt and decrypt data using separate keys. To exchange secure messages, there is no requirement for a pre-shared key. There is no shared secret between the two parties. The attacker must employ extremely long key lengths to carry out the attack. However, asymmetric encryption is 100 to 1000 times slower than symmetric encryption.

Symmetric encryption algorithms, also known as shared key algorithms, encrypt and decrypt data using the same pre-shared secret key. Because both parties are protecting a common secret, encryption methods can employ shorter key lengths. Asymmetric algorithms, on the other hand, are more computationally intensive than symmetric algorithms.

H. Backups

Documents can be stored in a various ways by using cloud technology. There is no need to create numerous files or other items. All files can be kept in one document using cloud technology. Storing critical data in the cloud can help to secure data against natural disasters, unauthorised modifications,and fires, among other things. After that, it can retrieve data. Documents are already being stored on the cloud. They store documents in a variety of methods. Dropbox, Google Drive,MEGA, Apple iCloud, etc...

VI CONCLUSION

Because of the data, databases are a popular target for cyber attackers. A database can be compromised in a many ways. A database should be safeguarded against numerous forms of attacks and threats. Most of the risks outlined above have countermeasures but some of them are effective while others are simply temporary. This study discusses the many attacks on the database and some cyber techniques for improving the database.

References

[1] Jain, S., & Chawla, D. (2020). A relative study on different database security threats and their security techniques. Int. J. Innov. Sci. Res. Technol., 5(5), 794-799.

[2] Kuner, C., Svantesson, D. J. B., H Cate, F., Lynskey, O., & Millard, C. (2017). The rise of cybersecurity and its impact on data protection. International Data Privacy Law, 7(2), 73-75.

[3] Markopoulou, D., Papakonstantinou, V., & De Hert, P. (2019). The new EU cybersecurity framework: The NIS

Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 105336.

[4] Angelini, M., Ciccotelli, C., Franchina, L., Marchetti-Spaccamela, A., & Querzoni, L. (2020, June). Italian National Framework for Cybersecurity and Data Protection. In Annual Privacy Forum (pp. 127-142). Springer, Cham.

[5] Sohail Imran, Irfan Hyder. (2009). Security Issues in Databases, Second International Conference on Future Information Technology and Management Engineering.

[6] Sarmah, S. S. (2019). Database Security–Threats & Prevention. International Journal of Computer Trends and Technology, 67(5), 46-53.

[7] Pevnev, V., & Kapchynskyi, S. (2018). Database security: threats and preventive measures.

[8] Prasad, R., & Rohokale, V. (2020). Mobile device cyber security. In Cyber security: the lifeline of information and communication technology (pp. 217-229). Springer, Cham.

[9] Wang, Y., Xi, J., & Cheng, T. (2021). The Overview of Database Security Threats' Solutions: Traditional and Machine Learning. Journal of Information Security, 12(01), 34.

[10] Poomari, A. SQL and Data Inference Injection and Enhancing Website Security, International Journal of Engineering Trends and Applications (IJETA) – Volume 7 Issue 5, Sep-Oct 2020

[11] Mubina Malik and Trisha Patel, Database Security - Attacks And Control Methods, International Journal of Information Sciences and Techniques (IJIST) Vol.6, No.1/2, March 2016

[12] Li, Y., Zhang, P., & Ma, L. (2019). Denial of service attack and defense method on load frequency control system. Journal of the Franklin Institute, 356(15), 8625-8645.

[13] Dharmakeerthi, T. D. A Study on Database Security Concerns and Resolutions (April 2020).

[14] Pill, M. (2019). 10 Database Attacks. ITNOW, 61(4), 42-43.

[15] Rijah, M. (2021). Security analysis, threats, & challenges in database.

[16] JFaragallah, O. S., Afifi, A., El-Shafai, W., El-Sayed, H. S., Naeem, E. A., Alzain, M. A., ... & Abd El-Samie, F. E. (2020). Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications. IEEE Access, 8, 42491-42503.

[17] Romanou, A. (2018). The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. Computer law & security review, 34(1), 99-110.